Office of the Chief Information Officer
Enterprise Policy

Policy Number: CIO-090 **Effective Date**: 03/05/2013

Subject: Information Security Incident Response Policy

Policy Statement: This policy identifies the necessity and procedures for agencies and COT to identify and notify appropriate personnel when a security incident occurs. Timely identification and notification of incidents allow COT and affected agencies to respond expeditiously to information security threats against Commonwealth resources. This policy also specifies events that may require special handling because of their potential impact or special reporting due to regulatory or other concerns.

Policy Maintenance: The Office of the CISO will be responsible for maintaining this policy. Agencies may choose to add to this policy, in order to enforce more restrictive internal policies as appropriate and necessary. Therefore, employees are to refer to their agency's security incident policies, which may have additional information or clarification of this enterprise policy.

Applicability: This policy shall be adhered to by all state and local entities and their users, including employees, contractors, consultants, temporaries, volunteers and other workers that connect to the Commonwealth's network and computing infrastructure.

Responsibility for Compliance: Each agency is responsible for assuring that employees within their organizational authority are aware of the provisions of this policy, that compliance by the employee is expected and that attempts to forego compliance with this policy may result in disciplinary action pursuant to KRS 18A up to and including dismissal. Agencies have the responsibility to enforce this policy. Failure to comply may result in additional shared service charges to the agency for COT's efforts to remediate information security incidents resulting from non-compliance with this policy. Moreover, all users of Commonwealth of Kentucky network and computing resources--including employees, contractors, vendors, and guests--shall be aware of what constitutes a security incident.

Definition:

Information Security Incident: An information security incident, as defined in National Institute of Standards and Technology (NIST) Special Publication 800-61, is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices. An incident response capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the exploited weaknesses, and restoring computing services.

Policy:

When agencies identify a potential security incident, they are required to contact the Commonwealth Service Desk (CommonwealthServiceDesk@ky.gov or (502) 564-7576) and to complete the COT-F012, Security Incident Report form (Security Incident Reporting Form, COT-F012). In the event that the incident is sensitive in nature, the reporting agency can contact the Security Administration Branch (COTSecurityServicesISS@ky.gov or (502)

564-1532) directly instead of the Commonwealth Service Desk. These actions allow the Office of the CISO to review the incident and determine the level of required involvement with the incident response. Depending on the scope of the incident and the skill set of the agency's personnel, COT's level of response may range from an advisory role to leading the investigation.

The Office of the CISO will review all incidents and, on a case-by-case basis, determine whether to become actively involved depending on the actual or potential expansion of the incident to other assets or agencies. COT will maintain confidentiality on any issues as regulations and policies permit. COT will work closely with agencies to coordinate activities with appropriate entities to recover from security incidents.

The Office of the CISO categorizes security incident handling into six phases:

1. Initial Notification and Assessment
2. Initial Response
3. Evidence Gathering
4. Remediation
5. Incident Assessment and Reporting
6. Post-incident Activities, to include Lessons Learned

Incident Response procedures can be a reaction to security activities such as the following:

- Unauthorized Access to Personnel, Data, or Resources
- Denial of Service Attacks
- Actual or Anticipated Widespread Malware Infections
- Data Breaches
- Loss/Theft of Commonwealth Equipment
- Significant Disruption of Services
- Significant Level of Unauthorized Scanning Activity to or from Hosts on the Network

Disclosure Communications: COT personnel will comply with all federal and state laws and policies for information disclosure to media or the public. COT will work closely with the management of affected agencies to ensure proper disclosure of security incident information. COT personnel will not disclose agency data or information related to security incident responses unless required to do so by state or federal regulations.

- Affected agencies must not disclose information about the security incident unless specifically required to do so by state or federal regulations. Such information includes network information, type of incident, specific infection type if applicable, number of assets affected, specific detail about applications affected, applications used to remediate/investigate, etc.

Physical Security Procedures: This policy does not cover physical security needs and threats, such as natural disasters, electrical outages, fire, or other physical threats to personnel or COT resources. Agencies are responsible for establishing and maintaining their own physical security procedures.

References:

- COT-F012, Security Incident Report form (Security Incident Reporting Form, COT-F012)
- KRS 42.724 , Creation and authority of Office of the Chief Information Security Officer
- NIST Special Publication 800-61, Computer Security Incident Handling Guide